AN ANALYSIS OF INFORMATION ASSURANCE RELATING TO THE DEPARTMENT OF DEFENSE RADIO FREQUENCY IDENTIFICATION (RFID) PASSIVE NETWORK

THESIS

Robert G. Giovannetti, First Lieutenant, USAF

AFIT/GIR/ENV/05M-05

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/05M-05

AN ANALYSIS OF INFORMATION ASSURANCE RELATING TO THE DEPARTMENT OF DEFENSE RADIO FREQUENCY IDENTIFICATION (RFID) PASSIVE NETWORK

THESIS

Presented to the Faculty

Department of Mathematics and Statistics

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Robert G. Giovannetti, BS

First Lieutenant, USAF

March 2005

AFIT/GIR/ENV/05M-05

AN ANALYSIS OF INFORMATION ASSURANCE RELATING TO THE DEPARTMENT OF DEFENSE RADIO FREQUENCY IDENTIFICATION (RFID) PASSIVE NETWORK

Robert G. Giovannetti, BS

First Lieutenant, USAF

Approved:

/signed/	14 March 2005
David D. Bouvin, Capt, USAF (Chairman)	date
/signed/	14 March 2005
Kevin L. Elder, Ph D. (Member)	date
/signed/	14 March 2005
Dennis D. Strouble, Ph. D. (Member)	date

Abstract

The mandates for suppliers to commence Radio Frequency Identification tagging set by Wal-Mart and the Department of Defense is changing this long-time rumored technology into reality. Despite the many conveniences to automate and improve asset tracking this technology offers, consumer groups have obstinately opposed this adoption due to the perceived weaknesses in security and privacy of the network. While the heated debate between consumers and retailers continues, little to no research has addressed the implications of security on the Department of Defense Radio Frequency Identification network. This thesis utilized a historical analysis of Radio Frequency Identification literature to determine whether the current network design causes any serious security concerns adversaries could exploit. The research concluded that at the present level of implementation, there is little cause for concern over the security of the network, but as the network grows to its full deployment, more evaluation and monitoring of security issues will require further consideration.

Acknowledgements

I would like to thank my advisor, Captain David D. Bouvin, and my readers, Dr. Kevin L. Elder and Dr. Dennis D. Strouble for their insight and guidance in this research. I am also grateful to the faculty, staff, and students within the information resource management program all helped and supported me though my time at the Air Force Institute of Technology.

I would also like to thank Dr. James Fales and Mr. Bruce Philpot and the rest of the staff at the Center for Automatic Identification at Ohio University for their help at the Automatic Identification & Data Capture Technical Institute conference.

Table of Contents

Page

Abstract iv

Acknowledgements v

Table of Contents vi

List of Figures viii

List of Tables ix

I. Introduction 1

Background 1
Problem 1
Research Question 2
Investigative Questions 2
Research Objective 2
Proposed Methodology 3
Scope and Limitations 3

II. Literature Review 5

Introduction 5
RFID Technology 5
Mandates on the Passive RFID Network 12
Information Assurance 17
Privacy Issues 24
Security Implications Unique for the DoD 27
Enhancing the Security of RFID 29
Chapter Overview 32

III. Methodology 33

Introduction 33
Research Methodology 33
Historical Research and MIS 35
Approach 35
Chapter Overview 37

IV. Analysis 38

Introduction 38
Investigative Questions 38
Research Question 42

Page

Chapter Overview 43

V. Conclusions 44

Introduction 44
Discussion 44
Recommendations 45
Limitations 46
Suggestions for Further Study 47
Chapter Overview 48

Appendix A: Glossary of Terms 49

Bibliography 50

Vita 55

List of Figures

Figure Page

1. An Implantable RFID Tag (VeriChip Corperation, 2004)..... 6
2. Michelin's RFID Tag for Tracking Tires ("Michelin Embeds RFID Tags in Tires," 2003) 7
3. Various Tag Designs ("RFID – The Technology," 2002) 7
4. RFID Microprocessors Next to An Ant (Meloan, 2003) 9
5. Example of EPC Tag Data Construct for 96-bit Tag Type 1 (EPCglobal, 2004). 15
6. Example of DoD 96-bit Tag Construct (The Under Secretary of Defense, 2004a, p. 2-8)..... 16
7. Areas of Information Assurance (Joint Pub 3-13, 1998, p. III-3)..... 19

List of Tables

Table Page

1. Bar code vs. Passive RFID (Accenture, 2001, p. 3) 10

2. Summary of RFID Tag Classes (Lewis, 2004, p. 9)..... 14

3. A Comparison of Two Historical Methodologies (Mason et al., 1997b; O'Brien et al., 2004) 37

An Analysis of Information Assurance Relating to the Department of Defense Radio Frequency Identification (RFID) Passive Network

I. Introduction

Background

Beginning in January of 2005, the Department of Defense (DoD) mandated that many classes of deliverables will have Radio Frequency Identification (RFID) microchips or tags that allow for automated tracking and identification through the supply chain. The majority of RFID systems currently in use today are stand-alone, and do not present much of a security concern. To fully automate the supply chain, universal standards have been developed to give each product manufactured for both the DoD and civilian industry a common protocol for identification. The RFID tags used within this network will consist of passive tags. The security concern with an open RFID network is that, although it will allow the automated tracking of individual pallets, cases, and eventually individual products, a third party could read the tags to gain insight into the movements of items moving within the DoD supply chain. This threat could give insight into operations or supply shortfalls.

Problem

As the DoD moves forward with the implementation of this new passive RFID network, it is very appealing to reap the benefits of improved inventories and supply chain management. However, unlike commercial applications, knowledge of movement

within the DoD supply chain could yield information regarding current or future military operations. The concern remains that as the DoD presses for implementation of the RFID passive network, possible security concerns could go unnoticed.

Research Question

Does present design of the DoD passive RFID network cause any serious security concerns that could be exploited by adversaries now or in the future?

Investigative Questions

To answer the research question, the following investigative questions are posed:

IQ1. How will the passive RFID network affect the five components of Information Assurance (IA)?

IQ2. What are possible methods for unauthorized people to gain information?

IQ3. What information will an adversary gain if he or she is able to read the data on the tag?

IQ4. What are potential options that could increase the security of the network should that become necessary?

Research Objective

The primary goal of this research is to provide a comprehensive review and analysis of the literature associated with the DoD passive RFID network and security to determine what affect this new network will present to the security of information. The research seeks to determine if this network presents serious security concerns that need

immediate attention. At the conclusion of the analysis, recommendations will offer suggestions for improving the security, if necessary.

Proposed Methodology

Historical analysis is the proposed methodology for this research. This form of research seeks to find patterns of events to determine how they are interrelated. It is also ideal due to its ability to interpret facts from the literature in context and achieve a synergy of two different bodies of literature, in this case, security and RFID. A framework specifically designed for historical analysis within the Management Information Systems (MIS) field guides the research. This framework, developed by Mason, McKenny, and Copeland, consists of a seven-step process to facilitate the research (1997a).

Scope and Limitations

The scope of this research is to look at the potential security issues specifically pertaining to the DoD passive RFID network. Since this network has yet to reach full implementation, many changes can still occur that will affect the security of the network. This research focuses on the security of the tags and readers of the passive RFID network. The back-end connections, where the readers communicate to the databases and software, were assumed secure since they will ride on the DoD intranet, which has strong security procedures, and it will resemble current applications riding on that network.

Historical research utilizes the researcher as the instrument of measure since the research relies on the researcher's ability to interpret the facts. The researcher's bias can

influence the findings of the research. Although the complete elimination of the bias is not possible, an objective consideration of sources and a close application of the research framework should minimize the bias.

II. Literature Review

Introduction

This chapter seeks to provide a comprehensive review of literature relating the DoD passive RFID network and security. Breaking this down further, this chapter outlines the technology, discusses privacy and security, and evaluates security-enhancing techniques to provide a clear picture of these different areas.

RFID Technology

The inception of RFID technology began in the late 1940's with aircraft transponders used to distinguish aircraft on radar (Ollivier, 1996). Radar technicians had difficulty identifying planes approaching as friendly or enemy, and if they were friendly, which radar signal corresponded to a plane or its pilot. Aircraft transponders send a specific code over radio frequency to allow radar operators to identify aircraft with the location indicated from the radar. This ability to send unique information over a radio frequency for another system to recognize is the fundamental trait common to all RFID systems. The further development of microprocessors and other technologies has allowed for increases in the capabilities and affordability of RFID, while decreasing the size and cost of the components. The RFID field is changing rapidly as technological advances enable a wide range of applications and capabilities.

In any application, the tag, the reader, and the back-end database are the three main components that make up an RFID system. A tag must contain at the very least a microchip that attaches to an antenna (some people consider the antenna to be a third

component). Tags come in a variety of shapes and sizes based on their application. The reader, often called the interrogator, sends a radio frequency signal to the tag, which replies with the tag's information. The reader then takes that information and, depending on the system, displays the information, shows an alert, or sends it to a database.

Many different designs and sizes exist for RFID tags, but the two primary types are active and passive. Active tags have a battery that allows them to work at distances ranging from about 100 meters to kilometers depending on antenna, power, and frequency (EPCglobal, 2004). The active tags are usually slightly larger and more expensive than passive tags since they need a battery and typically can perform more functions. Passive RFID tags consist of only a microchip and an antenna, and they draw power from the electromagnetic (EM) signal the reader transmits. That signal induces a current in the tag's antenna (EPCglobal, 2004). The figures below depict several different types of passive RFID tags.

Figure 1: An Implantable RFID Tag (VeriChip Corperation, 2004)

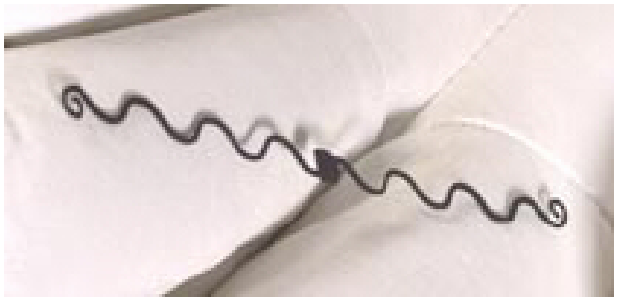

Figure 2: Michelin's RFID Tag for Tracking Tires ("Michelin Embeds RFID Tags in Tires," 2003)

Figure 3: Various Tag Designs ("RFID – The Technology," 2002)

The passive tags are typically smaller, cheaper and can last up to 20 years (Accenture, 2001). The passive tag works much like a mirror—it reflects the Radio Frequency (RF) energy from the EM signal, only the returning signal contains some sort of information, such as a serial number. Passive tags have a read range of about 3 meters depending on the reader and the antenna on the tag (EPCglobal, 2004). However, new designs in certain frequency ranges have enabled read distances under optimal conditions up to 15 meters (Cravotta, 2004). Another subtype of passive, called semi-passive also exists. Semi-passive tags have batteries that can be used for on board sensors, like temperature or pressure, or to assist in the read distance—they still rely on the reader field for communication, however (Lewis, 2004).

Tags also vary by the capability of being read-only or read-write. A read-write version can be changed or erased as tags progress through a supply chain or system. After the initial writing process, read-only tags do not allow changes to the information.

Since the tags communicate to the reader over a radio frequency, the frequency will determine many of the characteristics of the system. "The choice of operating frequency affects the reading distance, interference with other radio systems, communication data speed and antenna size. Low frequency systems typically use passive tags whereas higher frequency systems operate with active tags" (Accenture, 2001, p. 5). At lower frequencies, the antennas need to be larger, the data rates are slower, and the read range, the distance between the tag and the reader necessary for communication, is smaller. Higher frequencies need more line-of-sight between the tag and the reader because the higher EM waves do not pass through non-transparent objects as well as lower frequencies (2001). The operating frequency also complicates RFID networks because regions of the world allocate frequencies differently—a system utilizing a certain frequency here in the U.S. may find that its frequency is not compatible or approved for use in Europe or Japan. Five main operating frequencies for RFID networks exist globally, circa 130 kHz, 13.56 MHz, 860-960 MHz (UHF), 2.45 GHz, and 5.7GHz, but all are not necessarily available in all regions of the world (Delnicki, 2004). The UHF range is appealing because its typical read distance is between 6.4 and 7.0 meters, compared to about 0.5 meters for the frequencies lower than UHF and under 2.0 meters for the frequencies higher than UHF (2004). Different frequencies work better in different conditions and applications, so no one frequency is ideal in every situation.

By using different frequencies and advances in microchip technology, applications go far beyond the aircraft industry. RFID tags decreased in size—some are smaller than a grain of sand—this smaller size, coupled with decreasing costs and the ability to carry a significant amount of information make RFID an attractive option for many processes.

Figure 4: RFID Microprocessors Next to an Ant (Meloan, 2003)

Garage door openers and systems used to identify cars in case of theft are examples of applications for active tags we use everyday. The advances in passive tags have enabled drive through highway tolls, secure entry cards, and identification for livestock and pets. Passive tags have the potential for forgery prevention on gift certificates or even money (Takaragi, Usami, Imura, Itsuki, & Satoh, 2001, p. 45). The use of RFID technology is not new to the DoD. The "DoD currently operates the largest end-to-end active RFID system in the world…DLA [Defense Logistic Agency] and DDC [Defense Distribution Center] currently use active RFID tags on Air Lines of Communication (ALOC) pallets

and seavans that are sent to U.S. Central Command (CENTCOM)" (Walter-Groft, 2004, p. 10). The RFID technology proves useful in many applications, but the majority of systems utilizing RFID are close-looped as in the current system used by the DLA and the DCC. Close-loop, or stand-alone systems that utilize RFID typically operate only with themselves. For instance, a secure entry card operates only with the reader at the door; the format of the information or data communicated does not work with another system. The anticipated major application for RFID will be the implementation of RFID in the supply chain where it will operate as an open network with a common protocol.

Bar codes are instrumental as a data capture technique in nearly any application used to transfer data. The zebra pattern of bar codes is seen everyday, and the bar codes speed up consumer shopping, package shipping, and inventory tracking. RFID offers many advantages over bar codes, as the table below shows:

Table 1: Bar code vs. Passive RFID (Accenture, 2001, p. 3)

System	Barcode	RFID
Data Transmission	Optical	Electromagnetic
Typical Data Volume	1-100 Bytes	128-8K Bytes
Data Modification	Not possible	Possible
Position of Data Carrier for Read/Write	Visual contact	Non line of sight possible
Reading Distance	Several metres (line of sight)	From centimeters to meters (depending on the frequency and tags)
Access Security	Little	High
Environmental Susceptibility	Dirt	Very small
Anticollision	Not possible	Possible

Data transmission occurs optically with bar codes and through EM waves for RFID. The data volumes are similar for bar codes and RFID when looking at passive tags, but specialty systems for RFID have the capability to transfer significantly more data. Data modification, addressed earlier as read-write, remains an option for RFID. The scanner must "see" the bar codes for visual contact, while RFID tags pass information from within the packaging; the EM waves pass through most materials. Water and metal do not pass EM waves very well at most frequencies (Henning, Ladkin, & Sieker, 2004, p. 1; Sarma, Weis, & Engels, 2002, p. 465), but design considerations and packaging make it possible to use RFID (EPCglobal, 2004). The read distances for both bar codes and RFID are difficult to assess since both possess so many design considerations that affect read distance. Access security refers to the security of the data, and RFID has the ability to use authentication and encryption. This ability allows for protection of the data with passwords or for the encryption of the transmitted data. Bar codes are susceptible to environment damage that can render it unreadable; whereas, RFID tags remain readable against "dirt, frost, humidity, grease, and in the sunlight" (Accenture, 2001, p. 4). Finally, one of the most significant advantages of RFID is the advent of anti-collision. Anti-collision allows an RFID reader to read and/or write to multiple tags at one time, which is not possible for bar codes. Despite the many advantages RFID over bar codes, drawbacks do exist (2001).

The main element preventing RFID widespread use has been cost. In 2001, a cheap tag cost $0.50, but the ultimate goal for the RFID industry is to produce unique 64-bit or 96-bit, tags that cost $0.05 (Sarma, 2001). However, estimates that are more recent are encouraging. Alien Technology, an RFID developer, "does predict that in quantities

of 1 billion, RFID tags will approach 10 cents each, and in lots of 10 billion, the industry's holy grail of 5 cents" (McCullagh, 2003, p. 1).

Joe Dunlap, a supply chain specialist from Siemens Dematic, highlighted other concerns in addition to cost saying, "There will be exceptions where RFID tags fail or become damaged and human readable information is always required…If bar codes ever go away, it will be a long time from now" (Material Handling Management Staff, 2004, p. 24). RFID may not completely replace bar codes, as bar codes are cheap and will remain in use, but in many applications RFID can become the primary means of identification. According to the Military Marking for Shipment and Storage, MIL-STD-129P, unless otherwise specified in the contract, "identification bar code markings are required for DoD and contractor- or vendor- originated shipments" (Department of Defense Standard Practice, 2004, p. 46).

Mandates on the Passive RFID Network

On 4 June 2003, Wal-Mart directed that its 100 top suppliers would deliver all cases and pallets with RFID tags by 1 January 2005 (Barlas, 2003). The U.S. Department of Defense (DoD) followed Wal-Mart's lead and on 23 October 2003 also required that its top 100 vendors begin using RFID tags for tracking cases and pallets by January 2005 (Department of Defense, 2003). At the time of both mandates, no universal standards for interoperability existed for the data format on the RFID tags. Tom Torre, supply chain innovation group leader for Procter & Gamble, voiced his concerns stating, "Currently there are approximately 122 RFID protocols globally. They all work, but few work with each other" (Material Handling Management Staff, 2004, p. 24). The group in charge of

developing the standards for the RFID network is EPCglobal, Inc. EPCglobal is a joint venture between EAN-International (European Article Numbering Association) International and the Uniform Code Council (UCC) governed by a diverse board of key members (EPCglobal, 2004). EPC stands for Electronic Product Code, and it will be the standard for RFID; much the same as the bar code standard for the Universal Product Code (UPC). Their approach puts emphasis on:

> "Finding cheap, high performance tags and readers, making the electronic product code [EPC] a common language for everyone to use in the commercial supply chain, and finally, establishing the information network to form the data backbone of the system." (Material Handling Management Staff, 2004, p. 24)

Essentially, EPCglobal will direct the common language that the global RFID network will employ.

Another key player in the development of the passive RFID network will be the Association for Automatic Identification and Mobility, more commonly known as AIM Global. AIM Global "is a global trade association comprising providers of components, networks, systems, and services that manage the collection and integration of data with information management systems" (AIM Global, 2004, p. 2). AIM Global is the organization representing the manufacturers and service providers of RFID technology; their purpose is to solve the technological issues in the development of the passive RFID network.

In latest policy direction by the DoD released 30 July 2004, the rules for the implementation of passive RFID network is established (The Under Secretary of Defense,

2004a). Commencing on 1 January 2005, all case, pallet, and item packaging for packaged operational rations, clothing, individual equipment, tools, personal demand items, and weapon system repair parts and components delivered to the defense distribution depots of Susquehanna, PA and San Joaquin, CA will have RFID tags (2004a, p. 3-1). These tags will be within the approved frequency range, which is in the UHF range of 860-960 MHz, with a minimum read distance of three meters (2004a, p. 2-4). Furthermore, the tags will be EPC Class 0 and Class 1 tags (2004a, p. 1).

Table 2: Summary of RFID Tag Classes (Lewis, 2004, p. 9)

Class	Known as	Memory	Power Source	Application
0	EAS / EPC	None / EPC	Passive	Ant-theft / ID
1	EPC	Read -Only	Any	Identification
2	EPC	Read-Write	Any	Data logging
3	Sensor Tags	Read-Write	Semi-Passive/Active	Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc networking

Table 2 outlines each of the RFID tag classes and their applications. The "EAS" (electronic article surveillance) portion of the Class 0 tags, above, applies to tags used for theft prevention and contain no data on the tag. EAS tags simply notify the reader that a tag has passed it. Essentially the Class 0 and Class 1 tags utilized by the DoD passive network will remain read-only since they are factory programmed and can only be written once (Auto-ID Center, 2003, p. 10; Auto-ID Center, 2002, p. 7). By 1 January 2006, several more products delivered to nearly all the major defense depots will require RFID tags.

Two tag data formats or protocols are approved for the data on the tags: the DoD and the EPC tag data construct. The EPC tag data construct is appealing for manufactures that also deliver to the commercial supply chain since the manufacturers

can use one tag data construct for both DoD and commercial products. The DoD EPC network will support 64-bit and 96-bit tags, but the DoD directs transition to 96-bit tags "as soon as practicable" (The Under Secretary of Defense, 2004a, p. 2-9). The number of bits refers to the number of "1"s and "0"s actually on the tag, which represents the amount of space on the tag to write data. Figure 6, displays the format for the EPC 96-bit construct.

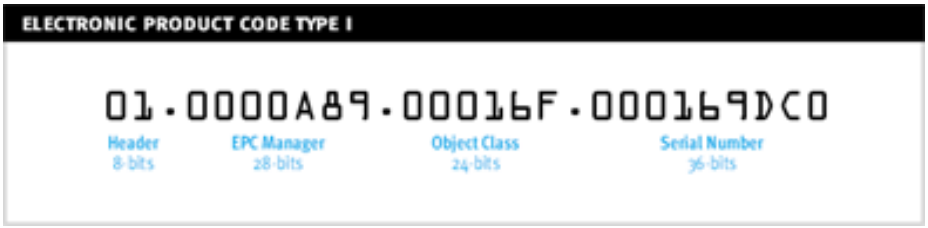

Figure 5: Example of EPC Tag Data Construct for 96-bit Tag Type 1 (EPCglobal, 2004)

The EPC format will provide the following types of information: the length, type, structure, version, and generation (Header), the entity responsible for maintaining the subsequent partitions of the EPC, which is usually the brand owner of the item or the company owning the location (EPC manager), the class of the item (Object Class), and finally a unique serial number (Serial Number). The EPC Manager of the EPC will be similar to an Internet Protocol (IP) address in computer networking. With 28 bits allocated for the EPC Manager, this allows for 2^28, or 268 million addresses for the manufacturers. Each manufacturer would have its own prefix, and allows for identify 2^24, or 16 million different prefixes for products in the object class portion. Finally, the serial number portion allows for 2^36, or 68 billion of each object class to be identified

uniquely. The capability for unique identification gives the government, commercial suppliers, and end-users the ability to track every item in the supply chain uniquely.

The DoD tag construct will resemble the EPC tag construct with a few differences. In figure 7, the 96-bit DoD construct is displayed:

Header	Filter	DODAAC/CAGE	Serial Number
8 bits	4 bits	48 bits	36 bits

Figure 6: Example of DoD 96-bit Tag Construct (The Under Secretary of Defense, 2004a, p. 2-8)

Under this construct, the header will be encoded "11001111," which will designate the tag as the DoD tag construct. The filter value will designate whether the tag is used for a pallet, case, or a Unique Identification (UID) item. The DODAAC/CAGE, also referred to as the Commercial and Government Entity (CAGE) code or the Government Managed Identifier, is a five-position alpha-numeric code, represented by 48 bits, which, "identifies the supplier and ensures uniqueness of serial number across all suppliers" (The Under Secretary of Defense, 2004c, p. 18). Finally, the serial number contains 36 bits to allow for 2^36 unique serial numbers under each CAGE code.

On 29 July 2003, the acting Under Secretary of Defense made UID a mandatory DoD requirement on all solicitations issued on or after 1 January 2004 (The Under Secretary of Defense, 2004b). UID is "the set of data for tangible assets that is globally unique and unambiguous ensures data integrity and data quality throughout life, and supports multi-faceted business applications and users" 2004b, p. 3). UID will be required for all contracts or delivery orders for tangible items if:

1. Unit acquisition cost is over $5,000
2. Item is serially managed

3. Item is mission essential
4. Item is controlled inventory
5. A consumable item or material where permanent identification is necessary (2004b, p. 9)

Linear and 2-dimenional bar codes can provide UID, but UID will be mandatory on RFID tags beginning 1 January 2007 (Department of Defense Standard Practice, 2004). RFID will be a key enabler for the UID program because it already has the capabilities for UID built into the tag data construct.

Information Assurance

Before discussing Information Assurance (IA), a proper definition is necessary. Information Assurance consists of:

> "Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." (DoD Directive 8500.1, 2002, p. 2)

In a working paper from the National Defense University on IA, the concerns over new commercial technologies were highlighted, "The introduction and adoption by industry of such new technologies as wireless, Voice Over Internet Protocol (VOIP), and Radio Frequency Identification Devices (RFID) are rapid, with little design concern for security and privacy" (Gansler & Binnenkijk, 2003, p. 3). The paper continues stating, "Introduction of this technology [wireless, VOIP, & RFID] in the commercial market is based on user acceptability, legal consequences, and bottom line cost analysis, not on

safety, potential loss of life, or national security policy considerations" (2003, p. 3). Specific problems were not explicitly identified, but the paper identifies the potential problem when technology developed commercially crosses into DoD applications. The passive RFID network does provide huge potential benefits for the DoD supply network, but this needs to be carefully balanced against the potential threats.

Joint Publication 3-13 discusses how joint forces will utilize Information Operations (IO) to support the national military strategy (Joint Pub 3-13, 1998, p. 2). The two major delineations of IO are offensive and defensive operations. Offensive IO involves utilizing resources to disrupt adversary decision makers or achieve certain objectives, while defensive IO aims to consolidate a host of techniques to "protect and defend information and information systems," (1998, p. viii). One of the primary methods of achieving defensive IO lies in the IA program. The DoD IA program:

> "Protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporation protection, detection, and reaction capabilities. IA employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software." (1998, p. III-1)

IA focuses on five areas to protect assets of the DoD. Figure 7, below highlights each of the five areas and provides a brief description.

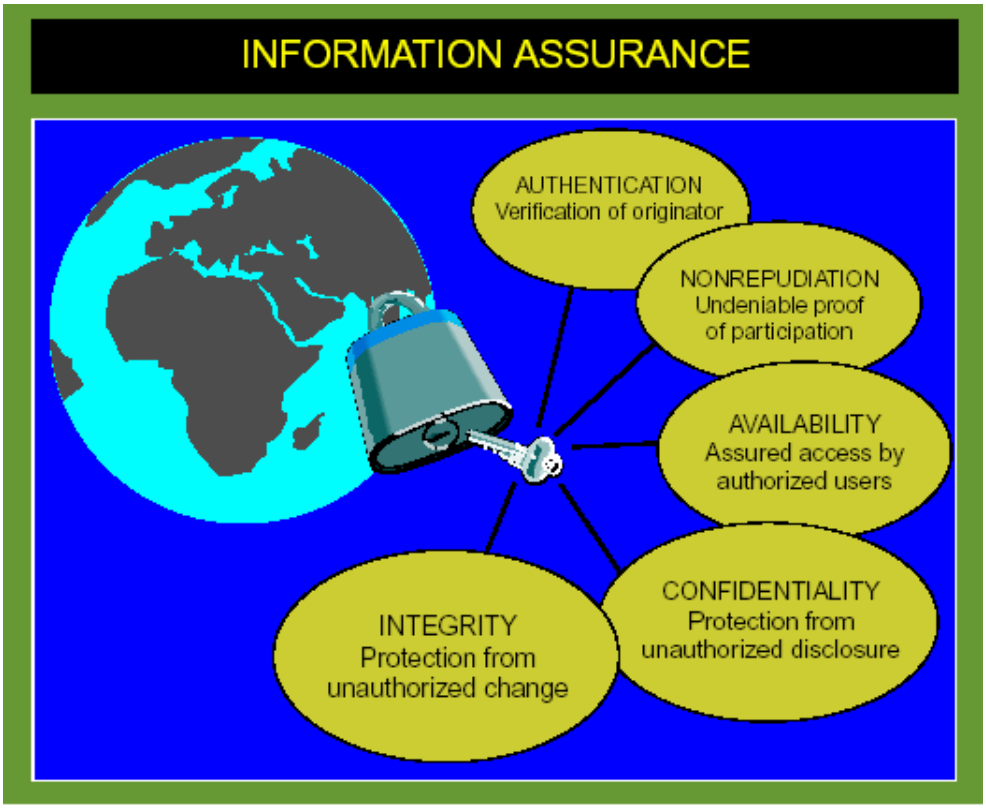

Figure 7: Areas of Information Assurance (Joint Pub 3-13, 1998, p. III-3)

Although this graphic provides a broad overview of the five elements of IA, more specific definitions are necessary to determine how they may affect the DoD passive RFID network. The definitions according to the DoD Directive 8500.1 and the National Security Telecommunications and Information Systems Instruction (NSTISSI) No. 4009, which serves as the National Information Assurance Glossary, are as follows:

- **Authentication**: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

- **Availability**: Timely, reliable access to data and information services for authorized users.

- **Integrity**: Quality of an IS [Information Systems] reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

- **Non-repudiation**: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

- **Confidentiality:** Assurance that information is not disclosed to unauthorized individuals, processes, or devices. (2002, pp. 17-22; 2003, pp. 4-44)

Before applying the components of IA to the DoD passive network, a restatement of a few factors of the network is necessary. All items shipped will possess shipping labels and bar codes in addition to RFID tags. The RFID tags will be Class 0 and Class 1, which means that they will be read-only. The databases that RFID utilizes to track inventory ride on a DoD intranet network. Kevin Ashton, Vice President of marketing of a reader manufacturer, stated that, "everything from the reader back is very standard internet infrastructure…so you have all the same security issues and opportunities that you have with the Internet" (Hulme & Claburn, 2004, p. 3). This analysis does not extend to possible vulnerabilities associated with the databases and software running on the DoD intranet. Since this portion of the network is standard internet infrastructure, the

analysis focuses on the portions of the RFID technology that is new and makes the network unique.

First looking at authentication, RFID will most likely enhance the security. In addition to bar codes, the RFID information on the tag will contain the manufacturer's data for verification to which manufacturer produced the product. Of course, this assumes initial programming occurred correctly. Spoofing tags is a threat that thieves or spies could attempt (Weis, Sarma, Rivest, & Engels, 2003) to threaten authentication. The spoofing of tags would require someone to change tag information or replace the original tag with a different one. Since the tags used in the network are read-only, changing tag information would only really become a threat if read-write tags were the standard. As for replacing a tag, this requires someone to physically remove the present tag and replace it with a spoofed tag. This scenario would present a much greater threat to the retail market for changing prices, should RFID become the primary means of check out at a store. This is still possible with the UPC bar codes, but switching UPC bar codes does not seem to be a widespread problem. An example of a government threat for spoofing would be if someone stole the contents of a pallet or case and delivered the container with the tag affixed. Upon delivery, the empty container and tag would show the item as delivered. Although plausible, spoofing does not currently pose a widespread or unique concern to the DoD passive network. The same scenario is just as possible with the bar code enabled network, and although it would go unnoticed for a little longer since it would show up as delivered. In addition, the physical tampering required to spoof a tag aids the security of the network. The spoofing of tags could be done to confuse the network, and although it would create confusion, the impact would be

limited, so it seems difficult to envision an example of why someone would do this or how this could pose a serious threat to the network. For the reasons discussed above, the threat of spoofing tags is not a serious threat to the network, and the benefit of verifying the tag information with the bar code and human readable information provides redundancy to enhance the component of authentication.

RFID should enhance the availability of the information since RFID will provide an additional method of data capture to bar codes and thus allow another way to obtain the information about the product. As RFID becomes the primary method of data capture, the potential for a denial-of-service attack could threaten the availability (Weis et al., 2003). The denial-of-service attack would have to interrupt communication between the reader and the tag or the reader and the database. Accomplishing this requires the placement of some sort of jamming device in proximity to the tag or the reader, or by killing the tags sometime before they reach their destination. Although this could be annoying, the bar codes will still be available as they provide an additional layer of redundancy should the RFID tags become unavailable. While the threat of a denial-of-service attack is possible, the added redundancy of RFID to bar codes should ultimately increase the availability of information.

Again, the redundancy of using both bar codes and RFID tags will also help the integrity of the data. Bar codes are reproducible from most any computer and printer (Hulme & Claburn, 2004), so tampering could occur. RFID tags are more difficult to reproduce and hiding them within the packaging will reduce tampering. Spoofing a tag could threaten the integrity of the information, but as addressed in the authentication

section, this threat appears minimal. In addition, a parity check between the information on the RFID tag and the bar code increases the ability to check the integrity of the data.

Utilizing RFID will probably be stronger against the threat of non-repudiation. The current databases used to track inventory with bar codes will either grow to incorporate RFID or will remain similar. The verification of the data being sent back and forth between the supplier and the DoD locations will most likely remain unchanged, but verifying the sender's identity and that the shipment was received is accomplished with less difficulty. The use of the serial numbers with RFID allows for would increase against non-repudiation since each item can be identified individually. Identification of individual cases allows receiving locations to determine exactly which cases were received and which are missing.

The element of confidentiality provides potential for larger problems. The protection of the tags from unauthorized reading could be a new cause of concern for the DoD. The main protection from confidentiality for the tag is the maximum read distance of 15 meters (Cravotta, 2004); although read distances most likely remain closer to the minimum read distance directed by the DoD at 3 meters (The Under Secretary of Defense, 2004a). According to the current design of the network, without encryption,

> "When queried by a reader, a tag sends the data to the reader using radio waves; the transmission is completely in the clear and the system has no inherent security. Further, any given reader can read just about any RFID tag, no matter who owns it. This can create security nightmares for companies worried about the privacy and integrity of their data." (Fisher, 2004, p. 1)

Therefore, once within a few meters, there remains no way to stop anyone from reading the tags, nor any way to know or record who, where, or when the tag was read.

RFID has possible implications on security. On one extreme, RFID will strengthen security as an additional data capture technique and will largely serve to benefit integrity, authentication, non-repudiation and availability. Spoofing and denial-of-service are potential attacks that could threaten authentication and availability, respectively. However, both are currently minimal threats as there is no real reason to spoof tags, and a denial-of-service would be inconvenient and limited in scope since it requires a physical local presence, but bar codes are still available should this occur. RFID tags offer another form of redundancy when combined with bar codes or human readable labels. The confidentiality aspect continues to be debated since the potential exists for propagation of large amounts of information without detection.

Privacy Issues

While the DoD may have concerns for the confidentiality of the passive RFID network, the commercial sector has been experiencing significant friction from privacy groups. The unfortunate drawback of RFID derives from the same attribute that makes it so useful—the ability to quickly pass unique information. According to privacy groups, tracking everything about anyone becomes too easy with RFID. Jeremy Wagstaff, a writer for the Far East Economic Review said it well,

> "What I don't want is an RFID tag on every product, banknote and stored-value card I have, transmitting information about me that allows shop clerks, bank tellers, policemen and my mother to know where I've been,

what I'm wearing, how much money I have in my pocket and what diseases I'm entertaining. That's not about to happen, but the technology allows for it. And some retailers would love it." (2003, p. 31)

The information collected from consumers like shopping habits and brand loyalty can be very valuable as Wagstaff alluded, and currently the developers of systems are the manufactures of the technology and the retailers or vendors—the public seems uninvolved and uninformed of the potential privacy invasions that could result. Beth Givens, director of the Privacy Rights Clearinghouse commented, "RFID is essentially invisible and can result in both profiling and locational tracking of consumers without their knowledge or consent" (Vijanyan, 2003, p. 5). Privacy activists were alarmed when Wal-Mart and Procter & Gamble tested RFID tags on lipstick in the summer of 2003. Webcams reportedly allowed researchers in Cincinnati to watch customers shopping for lipstick in Oklahoma (Bednarz, 2003, p. 10). The activists have worked to inform the public and slow the implementation of RFID. The group, CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering) organized numerous boycotts against retailers like Tesco and suppliers like Gillette (CASPIAN, 2005), and proposed legislation with the "RFID Right to Know Act of 2003" to "protect consumers against unwittingly purchasing products embedded with remote surveillance devices" (Albecht, 2005, p. 1). The concerns of CASPIAN and other groups caused legislators in Utah, California, and Missouri to attempt to pass legislation for retailers to inform consumers of tagged products (Collins, 2004a). Pro-RFID businesses claim that, "hypothetical scenarios of possible RFID abuses promoted by privacy groups are prompting the introduction of legislation to curtail the deployment of RFID before the technology has

ever been put to use" (2004, p. 1). Robert Atkinson, a vice president for the Progressive Policy Institute, says, the privacy groups are "spinning a whole set of worst-case scenarios" to scare the public and that, "In the past, after a technology, like bar coding, has been introduced, consumer concerns quickly abate" (2004, p. 1). The debate between privacy groups and Pro-RFID groups will almost certainly continue for a few years.

The concerns of the privacy groups center around the reading of tags on items a person is carrying. Although this could be severe under certain circumstances, the information collected would most likely relate to the clothes worn or items purchased from a store. The worst-case scenario may offend some people, but the result would probably resemble the hassles of spam E-Mail from advertisers or information collected from frequent buyer shopping cards. It seems that RFID tags, containing the information of a bar code with a serial number, should not cause people to fear for their personal safety. Regardless of one's stance on this issue or assessment of the vulnerability, the privacy groups have done a remarkable job of drawing attention to potential security concerns. A study by market intelligence company, BIGresearch, found that, "Nearly two thirds of RFID-aware adults are 'very concerned' or 'somewhat concerned' about [potential privacy] abuses" (Roberti, 2004b, p. 1). From the evidence suggested by the boycotts, legislation attempts, and surveys, the concerns of the privacy groups, whether they have merit or not, are effectively being heard by a segment of the consumer population.

Security Implications Unique for the DoD

Concerns for the government and military could mirror the privacy concerns voiced by the public. It seems logical to assume that any potential vulnerability experienced by the public, where the biggest concern is consumer privacy, would compound in severity in the DoD's realm of military operations. In order to keep RFID tags cheap for tracking a huge number of manufactured items, the current passive EPC data construct proposals and the DoD tag construct do not utilize encryption. Further, the DoD Directive, Number 8100.2, that establishes the policy for wireless devices, services, and technologies in the DoD Global Information Grid (GIG) explicitly states that, "Radio Frequency (RF) energy between RF identification tags, both active and passive, and the reader/interrogator does not require encryption" (2004, p. 2). Alan Estevez, assistant deputy undersecretary of defense for supply chain integration, provided two reasons why the network does not need encryption,

> "One reason is that the information on the passive tag is simply a serial number that means nothing until it's associated with information in a database, and the second reason is potential enemies should not be able to get close enough to read the tags." (Roberti, 2004a, p. 1)

He continued on the second reason stating that, "If we have people within 10 feet who are able to read a passive tag—or even 300 feet for an active tag—then we have bigger problems than them knowing what items are in our supply chain" (2004a, p. 1). The DoD cedes the fact that although unlikely, anyone with a RFID receiver with an 860-960 UHF frequency band capability and in close enough proximity can passively read any RFID tag. If the person can then couple the tag information, as Mr. Estevez alludes,

with the EPC Manager or the CAGE code, he or she would be able to calculate who made the product, and the serial and class codes could tell exactly what product passed the reader. The difficulty of coupling the tag information with what product it identifies remains unclear. The EPC Manager code is determined from the Object Name Service (ONS), which is a method of assigning manufacturers a unique code that they can then use as the prefix to assign product numbers and serial numbers under the object class and serial number fields. EPCglobal recently outsourced the management of the ONS directory to VeriSign, Inc. (Collins, 2004b). Beth Lovett, solutions marketing manager for VeriSign, expects that firewalls and access-management tools will ensure data remains safe from unauthorized parties on the EPCglobal network (Hulme & Claburn, 2004). The CAGE code for the DoD construct is managed by the DoD, and should be more difficult to access a database with all the codes listed. With either construct, once a company's EPC Manager code or CAGE code is available, the manufacturer will be obvious from reading the tag. The CAGE code is printed in the "From" address section of a Military Shipping Label (Department of Defense Standard Practice, 2004, p. 29), so although the CAGE code addresses are not available widespread in a database, they are certainly not viewed as sensitive information. Protection from unauthorized reading of the tags could then extend beyond the reaches of the military warehouse or even the base that they were located. Bottleneck locations, such as the commercial gates for entry or exit from a base could serve as collection points to read RFID tags.

Enhancing the Security of RFID

The fears consumer privacy groups identified have also become a concern of retailers and manufacturers in the realm of industrial espionage. Dan Bailey, an RFID architect at RSA Laboratories notes that, "Most RFID pilots have no security at all…It's almost like the early day of cell phones where no one paid attention to security. The system is all fine and good if you trust the reader, but if not, you have problems. People just haven't thought about this stuff" (Fisher, 2004, p. 1). Steve Lewis outlines three different methods in which industrial espionage could take place: Eavesdropping, where a listener can figure out tag numbers through the anti-collision methods of the reader, hiding readers along a supply chain, using hand held readers (2004). The first method of eavesdropping is unique because it involves unauthorized reading of the tags through the transmissions emitted by the reader. Since the reader transmissions are stronger than the tag's returning signal, obtaining the transmissions could occur from a much greater range than the tag can be read at, up to an approximate distance of 100 meters (Weis et al., 2003; Ranasinghe, Engels, & Cole, 2004). The other two possibilities involve simply reading and tracking the tags from a much closer range of a few meters.

Research found six different methods of enhancing security for a passive RFID network: physical security, the "kill tag" approach, the Faraday Cage, cryptography, silent tree walking, and blocker tags. Theoretically, the easiest way to protect an RFID network is to ensure that unauthorized people cannot enter a close enough proximity of any tags or readers to intercept any wireless transmissions. In actuality, this technique is difficult since the network encompasses the tags from the point of manufacture to

whenever they separate from the product. The physical security of DoD installations provides an enormous boost compared to corporate users.

The next method is the kill tag approach. This method offers protection to consumers by killing the tag upon purchase. Physically breaking the tag or sending it a kill command with a short 8-bit password will kill a tag (Juels, Rivest, & Szydlo, 2003). This technique is not a feasible option for the DoD since the tags need to remain active throughout the DoD supply chain to reap the benefits of RFID. The method, if fully utilized with retailers, should soothe consumers since they currently have no need for the tags to remain active after purchase.

The Faraday Cage method takes advantage of the inability of radio signals to pass through metal. A Faraday Cage is a metal mesh or foil that blocks the transmission between the tag and the reader (Juels et al., 2003). This technique could prove to be very effective for blocking certain tags that are more important, or it could serve to protect tags as they pass through a less secure environment. Ensuring products are shipped in metal containers will provide the same effect as a Faraday Cage, as the container will not allow radio frequencies to pass. Additionally, this technique is a very simple and cost effective method to protect tags from unauthorized reading.

Cryptographic methods are another way of increasing security. At the current cost designs for tags in the DoD and EPC tag protocols, "providing strong cryptographic primitives is currently not a realistic option" (Weis et al., 2003). Despite the limitations on the tags, cryptographic hash functions relying on the back-end, the reader and the database, increase the security of the network. One example of this is the hash-lock approach; the tags only release a simple form of identification for themselves termed the

"metaID." The metaID is sent to the reader that communicates with the database where it finds the corresponding key to the metaID. The reader sends the key information to the tag, and the tag then sends the information (Juels et al., 2003; Henrici & Müller, 2004; Weis et al., 2003). This method increases the security since accessing the information on the tag requires a key to unlock it, however, the metaID is unique, and so the tracking of the tag is still possible. Other derivations of hash functions designed to alleviate metaID tracking include randomized hash-locking (Weis et al., 2003) and hash-based identification variation (Henrici & Müller, 2004). Both have drawbacks as randomized hash-locking is scaleable to only a small number of tags and hash-based identification variation requires that the tags are read/write (Henrici & Müller, 2004). The use of hashing functions offers an increase in security through cryptography while maintaining the possibility for cheap tags. Incorporating cryptography into the DoD passive RFID network would require significant changes to the tags and the supporting databases.

As mentioned earlier, eavesdropping is a method of overhearing the transmissions sent from the reader to the tag to discern tag information. Anti-collision techniques allow readers to avoid data collision to collect the information from multiple tags that are simultaneously in the reader's coverage (Accenture, 2001). Tree-walking is a method of anti-collision, in which, the reader and tags within the reader field communicate bits back and forth to isolate tag information. Silent tree-walking is a security enhancing form of anti-collision where the reader does not rebroadcast the tag information, or will send "chaff" commands to confuse eavesdroppers, (Weis et al., 2003). Juels, Rivest, and Szydlo note that, "'silent tree-walking' and 'hash-lock' approaches for constructing 'smart' RFID tags…involve cryptographic operations on tags. Such approaches are thus

unlikely to be economically practical for the near future," (2003: 105-106). In spite of the current impracticality of these two techniques, they should remain open for consideration as the technology matures and costs become more feasible.

The final security enhancing technique evaluated is the blocker tag. Developed by RSA Security, the blocker tag is a passive tag placed in proximity to other tags that interferes with the tree-walking anti-collision technique by broadcasting both a "1" and a "0" bit simultaneously (2003). The affect is a denial-of-service on the reader as the tags passes through the reader's view (Hulme & Claburn, 2004). This technique would not cause any long-term effects on either the reader or other tags, but would cause tags in proximity to the blocker tag to become unreadable. This technique could benefit the security of the DoD passive network since it is an inexpensive and simple way to prevent unauthorized reading of tags. The blocker tag would need to be removed prior to use so that the DoD readers would receive the information. Unfortunately, the blocker tag could also be used in a malicious capability to cause a denial-of-service attack against the DoD network. While this is a much more severe threat to commercial check out applications, the blocker tag would need to remain physically within the reader's view.

Chapter Overview

This chapter evaluated RFID technology, described security and privacy implications, and offered techniques for improving the security of the DoD passive RFID network. This chapter will serve as the foundation for the evaluation of security in relation to the network.

III. Methodology

Introduction

This chapter introduces the basics of historical research, discusses the value historical research gives to the Management Information Systems (MIS) field, and explains the application of the methodology to the research problem and investigative questions.

Research Methodology

Searching for a methodology to answer the research and investigative questions proved to be more difficult than expected. The goal of the research is to provide a security assessment to a network that does not currently exist. The technology and layout have been determined, but changes will occur as it approaches full implementation across nearly all DoD installations. Despite the large amount of literature dealing with security of the public open EPC network, no peer reviewed literature was found relating security to the DoD passive RFID network. As O'Brien, Remenyi, and Keaney explain, "The object of academic research into business and management studies is to add something of value to the body of knowledge" (2004, p. 137). This research certainly seeks to add to the body of knowledge by analyzing the technical discipline of RFID with a security posture.

Several methodologies received consideration for the research. A case study methodology was an option, but without the full plan or deployment of the network, this would significantly reduce the scope of the research. Content analysis also had potential,

but due to the two separate bodies of knowledge, an element of context would have been lost. Historical research proved to be the research method of choice. Historical research, "considers the currents and countercurrents of present and past events, with the hope of discerning patterns that tie them all together…historical research deals with the meaning of events" (Leedy & Ormrod, 2000, p. 172). Certainly, establishing and evaluationing facts is important for any type of research, but for historical research, the goal is slightly different. Leedy & Ormrod explain, "The historical method is not, as with any other type of research, the accumulation of the facts, but rather the interpretation of the facts," (2000, p. 172). The interpretation of facts is the differentiating factor between historical and other methods or research. Interpreting the facts offers context into the subject of study.

> "Historiography can offer the business and management researcher an opportunity to acquire a rich understanding of situations and the context in which they exist. Knowing the background to any situation or to any issue enhances our comprehension and improves our ability to see what is important and what is not." (O'Brien et al., 2004, p. 135)

Therefore, insight into past events will allow an increased understanding of importance. Determining what is important and what is not, is the basis for making decisions. "Any understanding of a phenomenon or a situation will usually have to be based on a knowledge and appreciation of the trajectory of circumstances which have lead up to it" (O'Brien et al., 2004, p. 136). Past decisions are the result of past circumstances; so intuitively, all decisions currently made are the result of past circumstances. Therefore, "history helps endow knowledge with wisdom so that it can be used effectively by

leaders and decision makers," (Mason, McKenney, & Copeland, 1997a, p. 259). The ultimate goal of historical research is to interpret facts in context to allow for leaders and decision makers to make better decisions.

Historical Research and MIS

The technologies used around the world today are the result of past circumstances and decisions. "History provides the context within IS [Information Systems] phenomena occur. History allows the researcher to follow a trail and illuminates the role of decision making in shaping events," (Bannister, 2002, p. 7). Without the historical element, the intricate reasons for the decisions are not apparent. Mason, McKenney, and Copeland noticed this, "MIS researchers, for the most part, have not sought to identify fully the broad socio-economic conditions of continuity and change that accompany the use of information technology" (1997a, p. 258). The impacts of these decisions have determined how technology exists today. "Markets and basis of competition in an industry are changed—sometimes radically—by the decisions managers make when they select and invest in technology" (Mason et al., 1997a, p. 271). The goal of this research is to provide an interpretation of facts in context that will aid leaders and decision makers to make better decisions relating to security and the DoD passive RFID network.

Approach

Two historical methodologies received consideration for this research. The first was a framework developed by O'Brien et al. as a method for use in business and management studies. It is composed of a nine-step process. The nine steps are:

1. The Research Question
2. The Relevance Check
3. The Scope of the Research
4. Sources of Evidence
5. Assessment of Methods of Analysis
6. Assembling the Evidence
7. Developing the Story
8. Critiquing the Story
9. The Outcome of the Research (2004, pp. 138-141)

The design of second framework, developed by Mason et al., is specifically for application to MIS research. This framework consists of a seven-step process, and the steps are listed below.

1. Begin with Focusing Questions
2. Specify the Domain
3. Gather Evidence
4. Critique the Evidence
5. Determine Patterns
6. Tell the Story—the Account
7. Write the Transcript (1997b, pp. 312-317)

Although the two frameworks differ in the number of steps that they consist of, they are actually very similar. The table below demonstrates a comparison of how the researcher sees the two methodologies overlapping.

Table 3: A Comparison of Two Historical Methodologies (Mason et al., 1997b; O'Brien et al., 2004)

(Mason et al., 1997b)	(O'Brien et al., 2004)
1. Focusing Questions	1. The Research Question
	2. The Relevance Check
2. Specify the Domain	3. The Scope of Research
3. Gather the Evidence	4. Sources of Evidence
4. Critique the Evidence	5. Assessment of Methods of Analysis
5. Determine Patterns	6. Assembling the Evidence
	7. Developing the Story
6. Tell the Story	8. Critiquing the Story
7. Write the Transcript	9. Outcome of the Research

The theories certainly overlap in many areas. The process for conducting the research seems very similar with both methods: begin with questions, scope the research, gather evidence, evaluate the evidence, determine patterns, and produce some sort of an output of the research. For the purposes of this research, either methodology would accomplish the research effort, but ultimately, the Mason et al. framework was a better option as its specific development for MIS aligned better with the topic of research.

Chapter Overview

This chapter presented the methodological portion of the research by first defining historical research, highlighting the value it adds to the MIS area of study, and finally explaining the methodology chosen.

IV. Analysis

Introduction

The purpose of this research was to utilize historical analysis to evaluate potential security concerns or issues for the DoD passive RFID network as it exists today or as the design proposes for the future. The review of the literature completed in chapter II will serve as the evidence for the research and investigative questions.

Investigative Questions

IQ1. How will the passive RFID network affect the five components of IA?

Many different methods are available to assess security. The logical choice to assess the security of a DoD network was IA since it is one of the primary methods recommended for defensive IO in Joint Publication 3-13 (1998, p. III-1). The five components of IA, authentication, availability, integrity, non-repudiation, and confidentiality, provide a structure for analyzing the network. Although the potential threats of either spoofing or denial-of-service attacks could cause problems for authentication and availability, respectively, neither currently poses a serious threat. Spoofing involves changing or manipulating the information. As long as the tags are read-only on the network, the threat of spoofing an RFID tag is the same as switching out a bar code for a product. The main difference is that reproducing an RFID tag is slightly more difficult. While a denial-of-service attack would not allow the network to operate, it would have to occur from a close physical proximity, which should make it easier to identify, and the bar codes will remain an available method of data capture. For these

reasons, these two potential threats are not serious, and the passive RFID network either increased the security or caused no change for four out of the five components: authentication, availability, integrity, and non-repudiation. Adding RFID as another form of data capture provides more redundancy. This redundancy will enhance the security of authentication, availability, and integrity since a comparison of the two methods can provide a verification of the information on methods. The component of non-repudiation is enhanced since RFID allows for unique serial numbers for identification down to the case level. The analysis of the five components assumes that everything from the reader back, including databases, is standard software and hardware protected on the DoD intranet. The fifth component of confidentiality causes concern. The network allows for potential security issues since the information on the tags has little protection once any reader is within range. The information on the tags is susceptible to unauthorized access, and the tags have no capability to report the unauthorized reading by a third party.

IQ2. What are possible methods for unauthorized people to gain information?

Three methods an adversary could gain are eavesdropping, covertly hiding readers along the supply chain, and handheld readers. Eavesdropping attempts to take advantage of the stronger reader signal, which can extend up to 100 meters. Again, all communication between readers and tags occurs without encryption, so the readers allow for interception of information up to this distance. To gain the information, a device capable of intercepting the RF transmissions (like a computer with an antenna and appropriate software) is located within the broadcast range of the reader. The device would either store information locally or send the information over a network to another location. The device would focus on the anti-collision techniques of the reader to

determine which tags are passing the reader. The other two methods focus not on the reader, but on the reading of the tags. The maximum read distance for tags is 3 to 15 meters under optimal conditions. Hiding readers along the supply chain to record the passing of items requires placing a reader covertly within the supply chain. Bottleneck locations like installation gates or warehouses would be ideal to maximize the amount of information gained. Handheld readers are the final method evaluated for an adversary to gain information. This method requires a handheld reader and a person to get within the tag read range. Optical bar codes have this same vulnerability, but RFID allows non-line-of-sight reading at a rate of hundreds of reads per second (Weis et al., 2003). Theoretically, one person equipped with a handheld RFID reader could walk through a warehouse and collect the information from every tag. The last two methods for reading tags could occur anywhere the tag and product go, whether on or off an installation. These three methods are three likely scenarios in which an adversary could gain information from the RFID tags or readers.

IQ3. What information will an adversary gain if he or she is able to read the data on the tag?

The two different tag protocols authorized for the network increase the complexity of this question. It is unclear whether the EPC or the DoD tag protocols will become a majority on the network. The EPC protocol may have an advantage since suppliers can use the same construct for public distribution. The EPC protocol contains three main information areas of interest: the EPC manager, the object class, and the serial number. The DoD protocol also contains three main information areas of interest: the filter, the CAGE code, and the serial number. The filter value would tell how the

item was packaged and is found in the DoD specifications (The Under Secretary of Defense, 2004). The manufacturer is contained in the EPC manager, and the CAGE code for EPC and DoD constructs, respectively. Seeing the tag in a stream of bits does not mean that the manufacturer is readily apparent. The information needs pairing with EPC ONS information or DoD CAGE code information to determine what company received assignment of the unique value. Estimating the feasibility of this is extremely difficult. Currently this information is not readily available, but with the further propagation of the technology, it could become easier to pair since most do not consider the information sensitive. The product tag information is contained in the object class section of the EPC tag and the CAGE code or serial number for the DoD tag. The product information will differentiate between the products produced by the same manufacturer. Once the manufacturer has an approved range of prefixes for the EPC ONS, it can assign the product codes itself, so this information should be harder to ascertain than the manufacturer. In a worst-case scenario where the tag information yields the manufacturer and the product, the most information available for an adversary would place a certain product at a certain location at a certain time. For one product or shipment, this poses little threat, but the ability to monitor all shipments entering or exiting a warehouse, and installation, or multiple installations could pose a threat. However, the logistics required to covertly collect and track this information would parallel a conspiracy theory.

IQ4. What are potential options that could increase the security of the network should that become necessary?

Should more security become necessary in the future, the analysis of six different techniques (physical security, killing the tag, the Faraday Cage, cryptography, silent tree-walking, and blocker tags) proves a decent starting point. Of the six, killing the tag is probably the only technique that should not receive consideration since it disabling the tag defeats the purpose of RFID. Physical security and the Faraday Cage are two relatively inexpensive techniques currently used even if it is unknowingly. By keeping tags and readers away from the read distances, this denies the loss of information. DoD installations provide relatively good physical security. In addition, by transporting items in metal railcars or shipping containers, the interference of the metal on the radio signals helps to prevent unauthorized disclosure of information, which acts as a Faraday Cage. Focusing and refining these two techniques, along with a more thorough and strict policy could significantly improve the security of the network should that become necessary. The final three techniques, cryptography, silent tree-walking, and blocker tags, require increased tag and reader technology than what the minimal EPC and DoD tag constructs possess. These techniques will require more testing and further industry adoption before they are viable methods of enhancing security. The DoD should continue to consider and pursue these techniques as alternatives for increasing the security of the network.

Research Question

Does the present design of DoD passive RFID network cause any serious security concerns that could be exploited by adversaries now or in the future?

The network poses no serious security concerns to the four of the five components of IA. Confidentiality is the only component that has real potential for security concerns.

However, given the physical security of the DoD installations, the difficulty to pair tag information with the manufacturer and product, and the complexity required to collect and process a large volume of information, the confidentiality of the tags does not pose a serious security threat for the very near future. The confidentiality of the network remains a concern since the network does have the potential to yield large amounts of information regarding movement within the DoD supply chain. Security needs to remain a significant concern for the network to respond to this threat and others since the network is extremely dynamic and threats can surface quickly.

Chapter Overview

This chapter utilized the literature review of chapter II to answer the investigative and research questions for the research.

V. Conclusions

Introduction

This chapter summarizes the research effort. It will discuss the findings of the study, make recommendations, address limitations, and it will propose topics for future research.

Discussion

This study intends to draw increased attention to security associated with the DoD passive RFID network. Since this network remains in its infancy, changes to policy, technology, or design will be easier and cheaper than at any time in the future. The privacy concern witnessed in the consumer deployment of this technology should cause additional consideration for the DoD deployment. The typical concern of consumers is disclosure of personal information that subjects them to increases in advertising and marketing. In the military realm, disclosure of supply chain movement could give insight into operations that could jeopardize lives or mission success.

An additional observation made by the researcher was the polarization regarding security caused by the privacy debate in the consumer realm. The success of the privacy groups' concerns may have caused a backlash among the RFID community. The mention of eavesdropping on an RFID network seems to threaten the positive work and accomplishments of this revolutionary technology. This behavior is common to many Information Technology (IT) initiatives. IA is often an afterthought that can complicate

the initial design that was so painstakingly developed. Both sides of the debate will benefit to compromise and constructively entertain reasonable scenarios in the future.

Recommendations

This research concludes that the DoD passive RFID network currently does not pose any serious security threats, but security of the network should receive evaluation as the technology becomes ubiquitous. Weis et al. recommend that, "RFID-enabled environments should be equipped with devices to detected unauthorized read attempts or transmissions on tag frequencies" (2003, p. 10). This is a great idea that would enhance security, although deploying these devices to every RFID-enable site could be excessive. Despite the current lack of serious vulnerabilities, the potential still exists for threats to confidentiality in the future. The primary recommendation is to increase the monitoring for security vulnerabilities of this network. An organization must be responsible for the security of the network whether it is the offices pushing the implementation, the DoD Automatic Identification Technology (AIT) office and the service AIT offices or the emission security (EMSEC) program. According to the Air Force emission security instruction, AFI33-203, EMSEC is concerned with denying access to compromising emanations and "EMSEC mostly supports the 'confidentiality' requirement [of IA]" (2002, p. 4). This makes the EMSEC program the most logical choice for implementing security procedures. In either case, some organization must take ownership for ensuring the security of the network as more threats emerge. It is not enough to determine the network secure and continue without regard for the future.

Limitations

Historical analysis is unique because the researcher serves as the instrument of interpretation. One element of concern is the bias of the researcher. Borg and Gall addressed this writing, "the researcher's bias can affect the results as much in a laboratory experiment as in historical inquiry" (Borg & Gall, 1983, p. 801). A researcher's work within a similar field as a study, such as the IT field, causes some sort of bias. Although the elimination of researcher bias is not possible, it needs minimization through objectivity and dutiful application of the methodology.

This research involved the collection of a significant amount of literature. Books, peer-reviews journals, electronic databases, and websites all received thorough investigation for information pertaining to the subject. However, classified literature received no consideration for the purposes of this research, and sources of proprietary research were unavailable due to cost constraints.

Much of the literature surrounding passive RFID comes from a small community of experts. Many of the writers have their own biases or agendas toward the application of this new network or technology. To combat this, all points of view received consideration to better balance the extremes. Overall, the bias minimized as much as possible with additional weight given to sources that disputed multiple points of view.

This research looked specifically at the security of the communication between the tag and reader. This wireless transmission of information with an open protocol is what makes the passive DoD RFID network unique. The security of the databases and software utilized were not evaluated for two reasons. The first was that this is not yet standardized or ready for implementation. The second reason was because the databases

and software will ride on the DoD intranet, the intranet will provide security in a more traditional sense of IA related to computers and networks.

Another concern of the research was that both the technology and the literature were very dynamic. The open passive RFID networks for commercial companies and the DoD are undergoing constant changes. Without the network fully deployed, substantial changes can occur as issues arise. Shortfalls pointed out through this research can receive quick response, or may already been addressed.

Suggestions for Further Study

Suggestion #1: The Department of Defense's passive RFID network is only at its earliest stages of development. Currently only two receiving locations for the DoD require suppliers to provide RFID tags and that is only for a few classes of products. As the network expands to more locations, a case study looking at the specific security of one or a small number of these locations would provide valuable research. Although not necessary, the study would benefit from the use of commercial-off-the-shelf (COTS) readers to help search for vulnerabilities. A designed experiment would serve as an appropriate methodology for the study. The research would determine specific locations and methods that may be vulnerable to a certain installation.

Suggestion #2: All products traveling through the DoD supply chain are not equal in relation to defensive IO. The transportation of tanks and chemical warfare equipment probably yield more information into U.S. military operations than boots or office supplies. Research in the form of a survey or a Delphi study could help to

determine what products traveling through the supply chain need greater precaution for RFID security or any method of data capture.

Suggestion #3: The assumption surrounding RFID is a savings of time and money. Deploying this network has a cost to both the DoD and suppliers. Research quantifying the time or monetary savings could help determine whether the DoD is getting a sufficient return on investment (ROI). This research would help verify or disprove the assumption and discover if RFID tagging should continue down to the item level. The possible increase in accuracy or timeliness of the information would serve as additional factors for the study. A cost-benefit analysis is a feasible methodology for this research.

Chapter Overview

This chapter summarized the research effort. It restated the findings of the research, offered recommendations, highlighted limitations, and provided topics for future study.

Appendix A: Glossary of Terms

ALOC	Air Lines of Communication
CAGE	Commercial and Government Entity
CENTCOM	U. S. Central Command
COTS	Commercial of the Shelf Technology
DDC	Defense Distribution Center
DLA	Defense Logistic Agency
DoD	Department of Defense
DODAAC	Department of Defense Activity Address Code
EAN	European Article Numbering
EM	Electromagnetic
EMSEC	Emission Security
EPC	Electronic Product Code
GIG	Global Information Grid
IA	Information Assurance
IO	Information Operations
IT	Information Technology
MIS	Management Information Systems
NSTISSI	National Security Telecommunications and Information Systems Instruction
ONS	Object Name Service
RF	Radio Frequency
RFID	Radio Frequency Identification
ROI	Return on Investment
UCC	Uniform Code Council
UHF	Ultra High Frequency
UID	Unique Identification
UPC	Universal Product Code
VOIP	Voice Over Internet Protocol

Bibliography

Accenture. (2001, November 30). Radio Frequency Identification (RFID). White Paper. [Online] Retrieved 26 February 2004, from http://www.accenture.com/xdoc/en/services/technology/vision/RFIDWhitePaperNov01.pdf

Aim Global. (2004). About Us. *Aim Global Website*. [Online] Retrieved 5 November, 2004. http://www.aimglobal.org/aboutaim/

Albecht, K. (2003, June 11). Consumer Group Unveils RFID Labeling Legislation. [Online] Retrieved 9 February 2005, from http://www.spychips.com/press-releases/right-to-know-release.html

Auto-ID Center. (2002, November 14). 860-MHz-960MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Recommended Standard. Technical Report, Version 1.0.1. [Online] Retrieved 2 November 2004, from http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

-----. (2003, February 23). Draft Protocol Specification for a 900 MHz Class 0 Radio Frequency Identification Tag. Technical Report. [Online] Retrieved 2 November 2004, from http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

Bannister, F. 2002. The Dimension of Time: Historiography in Information Systems Research. *Electronic Journal of Business Research Methods*. 1(1): pp. 1-10.

Barlas, D. (2003, June 4). Wal-Mart's RFID Mandate. *Line 56*. http://www.line56.com/articles/default.asp?ArticleID=4710

Bednarz, A. (2003, November 24). Legislator Raises RFID Privacy Flag. *Network World*, Framingham: 20(47), p. 10.

Borg, W. & Gall, M..D. *Educational Research: An Introduction*. (4th Ed.) Longman, 1983.

CASPIAN. (2005). Stop RFID Website. [Online] Retrieved 9 February 2005, from www.spychips.com

Cravotta, N. (2004, May 27). RFID IC Avoids Collisions, Reads at Greater-than-15m Distances. EDN, Boston. 49(11), p. 20.

Collins, J. (2004a, October 11). Think Tank Progressive Policy Institute Says that Inaccurate Scenarios of Possible RFID Abuses are Prompting the Introduction of

Premature Legislation. *RFID Journal*. [Online] Retrieved 2 November 2004, from http://www.rfidjournal.com/article/articleprint/1183/-1/1/

-----. (2004b, September 29). VeriSign Initiates Two EPC Services. *RFID Journal*. [Online] Retrieved 2 November 2004, from http://www.rfidjournal.com/article/articleprint/1140/-1/1/

Delnicki, R, Senior Project Manager, Uniform Code Council (UCC). Briefing at the Automatic Information Data Capture Technical Institute. EPC 101—In the Beginning There Was an Idea…, Ohio University, Athens, OH, 27 July 2004.

Department of Defense. (2004, April 14). Directive 8100.2: Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG). Retrieved 2 November 2004, from http://www.dtic.mil/whs/directives/corres/pdf/d81002_041404/d81002p.pdf

-----. (2002, October 24). Directive 8500.1: Certified Current as of November 21, 2003. [Online] Retrieved 2 November 2004, from http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf

-----. (2003, October 23). DOD Announces Radio Frequency Identification Policy. News Release. http://www.defenselink.mil/releases/2003/nr20031023-0568.html

Department of Defense Automatic Identification Technology Office. (2004, June). Unique Identification 101—The Basics. http://www.dodait.com/rfid/07012004/DOD%20Tag%20data%20constructs.pdf

Department of Defense Standard Practice. (2004, October 29). Military Marking for Shipment and Storage MIL-STD-129P w/CHANGE 3. http://www.acq.osd.mil/log/logistics_materiel_readiness/organizations/sci/rfid/assetts/MIL-STD-129P-chg3-29Oct04%20(2).pdf

EPCglobal. (2004). About the Technology. *EPCglobal Website*, Retrieved February 5, 2004. http://archive.epcglobalinc.org/aboutthetech_indepthlook2.asp

Fisher, D. (2004, June 14). "RSA Service Targets RFID Security." *eWeek*. [Online] Retrieved 13 Oct 2004, from http://www.eweek.com/article2/0,1759,1612105,00.asp

Gansler, J. & Binnendijk, H. (2003, May). Information Assurance: Trends in Vulnerabilities, Threats, and Technologies—Working Paper. *National Defense University*. http://www.ndu.edu/ctnsp/IAverMay03.pdf

Henning, J. E., Ladkin, P. B., & Sieker, B. (2004, October 28). Privacy Enhancing Technology Concepts for RFID Technology Scrutinised. RVS Group, University of Bielefeld, Germany. http://www.rvs.uni-bielefeld.de/cms/publications/RVS-RR-04-02

Henrici, D. & Müller, P. (2004). Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. *PerCom Workshops*, IEEE Computer Society, 2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), 14-17 March 2004, Orlando, FL, USA, pp. 149-153.

Hulme, G. V. & Claburn, T. (2004, Nov 15). RFID's Security Challenge. *InformationWeek*. http://www.informationweek.com/story/showArticle.jhtml?articleID=52601030

Joint Chiefs of Staff. (1998, October 9). Joint Doctrine for Information Operations. Joint Pub 3-13. United States Department of Defense. http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

Juels, A., Rivest, R. L., & Szydlo, M. (2003). The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pp. 103-111. ACM Press. 2003

Leedy, P. D. & Ormrod, J. (2000). *Practical Research: Planning and Design*. (7th Ed.) NY: Prentice Hall.

Lewis, S. (2004, Jan). "A Basic Introduction to RFID Technology and Its Use in the Supply Chain." *Laran RFID*. White Paper. http://www.idii.com/wp/LaranRFID.pdf

Mason, R. O., McKenney, J. L., & Copeland, D.G. (1997a). Developing an Historical Tradition in MIS Research. *MIS Quarterly*: September, pp. 257-276.

-----. (1997b). An Historical Method for MIS Research: Steps and Assumptions. *MIS Quarterly*: September, pp. 307-320.

Material Handling Management Staff. (2003, December). RFID: Wal-Mart Has Spoken. Will You Comply? *Material Handling Management*. Cleveland, 58(13), p. 24.

McCullagh, D. (2003, January 13). RFID Tags: Big Brother in Small Packages. *CNet News.com*. [Online] Retrieved January 23, 2004, from http://news.com.com/2010-1069-980325.html

Meloan, S. (2003). Toward a Global 'Internet of Things. *Sun Developer Network*. [Online] Retrieved 26 January 2005, from http://java.sun.com/developer/technicalArticles/Ecommerce/rfid/

Michelin Embeds RFID Tags in Tires. (2003). *RFID Journal*. Article posted 17 Jan 03. [Online] Retrieved 22 Sep 04, from http://www.rfidjournal.com/article/articleview/269/1/1/

National Security Telecommunications and Information Systems Instruction (NSTISSI) No. 4009. (2003, May). National Information Assurance (IA) Glossary. [Online] Retrieved 28 January 2005, from http://www.nstissc.gov/Assets/pdf/cnssi_4009.pdf

Ollivier, M. M. (1995). RFID—A Practical Solution for Problems You Didn't Even Know You Had! *The Institution of Electrical Engineers*, Savory Place, UK.

Ranasinghe, D. C., Engels, D. W., & Cole, P. H. (2004). Security and Privacy: Modest Proposals for Low-Cost RFID Systems. Paper presented at Auto-ID Labs Research Workshop, 23 September 2004. [Online] Retrieved 28 January 2005, from http://www.m-lab.ch/auto-id/SwissReWorkshop/papers/SecurityAndPrivacy-ModestProposalsForLowCostRFIDsystems.pdf

"RFID – The Technology." (2002). *High Tech Aid Website*. http://www.hightechaid.com/tech/rfid/rfid_technology.htm

Roberti, M. (2004a, August 9). DoD Releases Final Policy. *RFID Journal*. [Online] Retrieved 2 November 2004 from http://www.rfidjournal.com/article/articleprint/1080/-1/1/

-----. (2004b, October 22). Consumer Awareness of RFID Grows. *RFID Journal*. [Online] Retrieved 2 November 2004 from http://www.rfidjournal.com/article/articleprint/1202/-1/1/

Sarma, S. E. (2001). Towards the 5 Cent Tag. *MIT Auto-ID Center White Paper-006*.

Sarma, S. E., Weis, S. A., & Engels D. W. (2002). RFID Systems and Security and Privacy Implications. Paper presented at Cryptographic Hardware and Embedded Systems—CHES 2002, 4th International Workshop, Redwood Shores, CA, USA, August 13-15, 2002. Edited by Burton Kaliski, Jr, Cetin Koc, and Christof Paar. *CHES 2002, LNCS 2523*. Springer-Verlag, Berlin 2003, pp. 454-469.

Takaragi, K., Usami, M., Imura, R., Itsuki, R., & Satoh, T. (2001, November/December). An Ultra Small Individual Recognition Security Chip. *IEEE Micro*, 21(6), pp. 43-49.

The Under Secretary of Defense. (2004a, July 30). Radio Frequency Identification (RFID) Policy. http://www.dodait.com

-----. (2004b, June). Unique Identification 101—The Basics. http://www.acq.osd.mil/dpap/Docs/uid/UID%20101.pdf

-----. (2004c, November 30). United States Department of Defense Suppliers' Passive RFID Information Guide. Version 3.0 http://www.dodait.com

The United States Air Force. (2002, September 26). AFI33-203—Emission Security. [Online] Retrieved 15 February 2005, from http://www.e-publishing.af.mil/pubfiles/af/33/afi33-203/afi33-203.pdf

VeriChip Corperation. (2004). Company Website. [Online] Retrieved 27 Jan 05. http://www.adsx.com/prodservpart/verichip.html

Vijayan, J. (2003, September 1). Use of RFID Raises Privacy Concerns. *Computerworld*, Framingham, 37(35), p. 5.

Wagstaff, J. (2003, August 7). Eyes on You, the Shopper. *Far Eastern Economic Review*, 166(31), p. 31.

Walter-Groft, J. (2004, April). DDC to Expand Uses for RFID. *DDC News*. Spring 2004, p. 10. http://www.ddc.dla.mil/review/Spring2004/10.pdf

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2003). Security and Privacy Aspects of Low-Cost Radio Identification Systems. *First Internation Conference on Security in Pervasive Computing, 2003*. [Online] Retrieved 28 January 2005, from http://theory.lcs.mit.edu/~sweis/spc-rfid.pdf

Vita

First Lieutenant Robert Gene Giovannetti graduated from Badger High School in Lake Geneva, Wisconsin. He entered undergraduate studies at the United States Air Force Academy in Colorado Springs, Colorado where he graduated with a Bachelor of Science degree in operations research with a minor in mathematics in May 2001.

His first assignment was to Spangdahlem Air Base, Germany as a communications officer where he served as an Aerospace Communications-and-Information Expertise (ACE) Lieutenant. In August 2003, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to the 552nd Communications Group at Tinker Air Force Base, Oklahoma. He is engaged to 1Lt Jennifer Glomb who is an aerospace physiologist at Tinker, AFB.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
21-03-2005	Master's Thesis	Sept 2003-Mar 2005

4. TITLE AND SUBTITLE

An Analysis of Information Assurance Relating to the Department of Defense Radio Frequency Identification (RFID) Passive Network

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Giovannetti, Robert G., First Lieutenant, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 641
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/05M-05

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Lt Col Clifton Poole
Information Assurance Laboratory
Information Resource Management College
National Defense University
Ft. McNair, Washington, D.C. 20319-5066

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The mandates for suppliers to commence Radio Frequency Identification tagging set by Wal-Mart and the Department of Defense is changing this long-time rumored technology into reality. Despite the many conveniences to automate and improve asset tracking this technology offers, consumer groups have obstinately opposed this adoption due to the perceived weaknesses in security and privacy of the network. While the heated debate between consumers and retailers continues, little to no research has addressed the implications of security on the Department of Defense Radio Frequency Identification network. This thesis utilized a historical analysis of Radio Frequency Identification literature to determine whether the current network design causes any serious security concerns adversaries could exploit. The research concluded that at the present level of implementation, there is little cause for concern over the security of the network, but as the network grows to its full deployment, more evaluation and monitoring of security issues will require further consideration.

15. SUBJECT TERMS
Radio Frequency Identification, RFID, Security, Information Assurance

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
REPORT	**ABSTRACT**	**c. THIS PAGE**			David D. Bouvin, Capt, USAF
U	**U**	**U**	**UU**	66	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4742; david.bouvin@afit.edu